PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-251155
(43)Date of publication of application : 27.09.1996

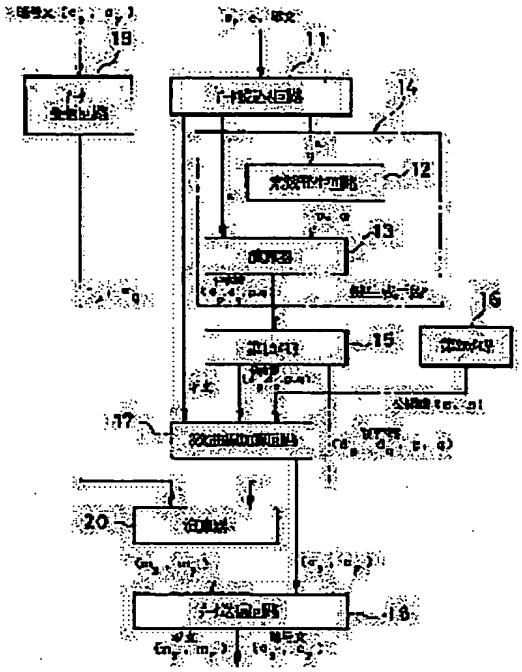
(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 07-048575
(22)Date of filing : 08.03.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KOYAMA KENJI

(54) CIPHERING DEVICE, DECIPHERING DEVICE, CIPHERING AND DECIPHERING DEVICE AND CIPHER SYSTEM

(57)Abstract:
PURPOSE: To provide a ciphering device and a cipher system particularly excellent in the deciphering speed as compared with RSA ciphers in use.
CONSTITUTION: This device is provided with a key generation means 14 which generates primes p and q and at the time of computation with dp and dq satisfying dp=(1/e)mod(p-1), dq=(1/e)mod(q-1), where an integer e is mutually prime with the least common multiple of the product n=pq, (p-1) and (q-1), sets the product n and an integer e to be public keys and sets the primes p, q and dp, dq to be secret keys. In addition the device is provided with a ciphering calculation means which makes an integer pair of inputted plain texts correspond to a point on a cubic curve, determines a point obtained by e-folding the point by the use of the public keys by arithmetic on the cubic curve, and outputs arithmetic results as a cipher text, and a deciphering arithmetic means which subjects the integer pair of the inputted cipher text to homomorphic transformation, then raises the result to the dp-th power under a divisor p and dq-th power under a divisor q, and synthesizes them by the use of the Chinese remainder theorem to output a plain text.



LEGAL STATUS

[Date of request for examination]	08.03.1995
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2624634
[Date of registration]	11.04.1997
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

Copyright (C); 1998,2003 Japan Patent Office

Japanese Publication for Unexamined Patent Application

No. 8-251155/1996 (Tokukaihei 8-251155)

A. Relevance of the above-identified Document

This document has relevance to claims 1, 2, and 6 to 13 of the present application.

B. Translation of the Relevant Passages of the Document

See the attached English Abstract.

(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－251155

(43)公開日　平成8年(1996)9月27日

(51)Int.Cl.⁶		識別記号	庁内整理番号	FI			技術表示箇所
H04L	9/06			H04L	9/02	Z	
	9/14		7259－5J	G09C	1/00		
G09C	1/00						

審査請求 有　請求項の数4　OL　（全 7 頁）

(21)出願番号　特願平7－48575

(22)出願日　平成7年(1995)3月8日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者　小山　雄二
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

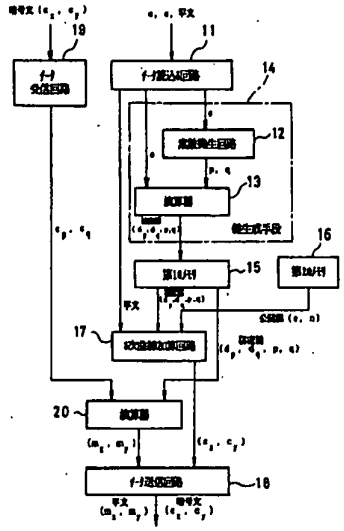
(74)代理人　弁理士　三好　秀和　（外1名）

(54)【発明の名称】　暗号装置および復号化装置および暗号・復号化装置および暗号システム

(57)【要約】

【目的】　本発明は、従来のＲＳＡ暗号に比べたとき、特に復号化速度に優れた暗号装置および暗号システムを提供することを目的とする。

【構成】　素数ｐとｑとを生成して、これらの積ｎ＝ｐｑと、（ｐ－１）および（ｑ－１）の最小公倍数Ｎと、この最小公倍数Ｎと互いに素な整数ｅに対し、$d_p = (1/e) \mod (p-1)$，$d_q = (1/e) \mod (q-1)$を満たすd_p，d_qと演算したときの、積ｎと整数ｅとを公開鍵とすると共に、素数ｐとｑおよび前記d_pとd_qとを秘密鍵とする鍵生成手段と、入力される平文の整数対を３次曲線上の点と対応させ、この点を前記公開鍵を用いてｅ倍した点を前記３次曲線上の演算で求め、この演算結果を暗号文として出力する暗号化演算手段と、入力される暗号文の整数対を準同形変換した後に、法ｐのもとでd_p乗および法ｑのもとでd_q乗して、それらを中国人の剰余定理で合成して平文を出力する復号化演算手段とを備えて構成される。



(2)

1

【特許請求の範囲】

【請求項１】　素数ｐとｑとを生成して、これらの積ｎ＝ｐｑと、（ｐ－１）および（ｑ－１）の最小公倍数Ｎと、この最小公倍数Ｎと互いに素な整数ｅに対し、$d_p = (1/e) \mod (p-1)$，$d_q = (1/e) \mod (q-1)$を満たすd_p，d_qと演算したときの、積ｎと整数ｅとを公開鍵とすると共に、素数ｐとｑおよび前記d_pとd_qとを秘密鍵とする鍵生成手段と、入力される平文の整数対を３次曲線上の点と対応させ、この点を前記公開鍵を用いてｅ倍した点を前記３次曲線上の演算で求め、この演算結果を暗号文として出力する暗号化演算手段とを有することを特徴とする暗号装置。

【請求項２】　素数ｐとｑとを生成して、これらの積ｎ＝ｐｑと、（ｐ－１）および（ｑ－１）の最小公倍数Ｎと、この最小公倍数Ｎと互いに素な整数ｅに対し、$d_p = (1/e) \mod (p-1)$，$d_q = (1/e) \mod (q-1)$を満たすd_p，d_qと演算したときの、積ｎと整数ｅとを公開鍵とすると共に、素数ｐとｑおよび前記d_pとd_qとを秘密鍵とする鍵生成手段と、入力される暗号文の整数対を準同形変換した後に、法ｐのもとでd_p乗および法ｑのもとでd_q乗して、それらを中国人の剰余定理で合成して平文を出力する復号化演算手段とを有することを特徴とする復号装置。

【請求項３】　素数ｐとｑとを生成して、これらの積ｎ＝ｐｑと、（ｐ－１）および（ｑ－１）の最小公倍数Ｎと、この最小公倍数Ｎと互いに素な整数ｅに対し、$d_p = (1/e) \mod (p-1)$，$d_q = (1/e) \mod (q-1)$を満たすd_p，d_qと演算したときの、積ｎと整数ｅとを公開鍵とすると共に、素数ｐとｑおよび前記d_pとd_qとを秘密鍵とする鍵生成手段と、入力される平文の整数対を３次曲線上の点と対応させ、この点を前記公開鍵を用いてｅ倍した点を前記３次曲線上の演算で求め、この演算結果を暗号文として出力する暗号化演算手段と、入力される暗号文の整数対を準同形変換した後に、法ｐのもとでd_p乗および法ｑのもとでd_q乗して、それらを中国人の剰余定理で合成して平文を出力する復号化演算手段とを有することを特徴とする暗号・復号化装置。

【請求項４】　送信元から送信される平文の整数対を３次曲線上の点と対応させ、これを送信元の公開鍵との乗算を当該３次曲線上の演算で行なって暗号化する暗号化手段と、この暗号化手段で暗号化された暗号文を前記送信元へ送信する送信手段と、この送信手段を介して送信された暗号文を受信する受信手段と、この受信手段を介して受信した暗号文に対し、自己の秘密鍵による巾乗算を行なって復号化する復号化手段とを有することを特徴とする暗号システム。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は通信の機密保護をはかり、通信文の改ざんの有無を確認するために用いられ、暗号鍵を公開とする暗号装置および復号化装置および暗号・復号化装置および暗号システムに関する。

【０００２】

【従来の技術】従来から通信におけるデータ等の盗聴、改ざんおよび破壊等がシステムを守るためにデータの暗号化が行われる。この暗号化方式には、大別して慣用暗号方式と公開鍵暗号方式が知られる。このうち公開鍵暗号方式とは利用者毎に予め生成された暗号化鍵である公開鍵と復号鍵である秘密鍵とを用いて暗号化及び復号を行なう暗号化方式である。通常、公開鍵は通信ネットワーク上で公開され、秘密鍵は鍵を生成した利用者自身により秘密とされることから、鍵管理が容易である。この公開鍵暗号方式の代表的なアルゴリズムとしてＲＳＡ暗号（R. L. Rivest, A. Shamir and L. Adleman, :A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol. 21, No. 2, pp. 120－126, 1978）がある。

【０００３】

【発明が解決しようとする課題】しかしながら、上述したＲＳＡ暗号化方式は復号化速度が遅く改善が望まれていた。

【０００４】本発明は、上記課題に鑑みてなされたもので、従来のＲＳＡ暗号に比べたとき、特に復号化速度に優れた暗号装置および復号化装置および暗号・復号化装置および暗号システムを提供することを目的とする。

【０００５】

【課題を解決するための手段】上記目的を達成するため本願第１の発明は、素数ｐとｑとを生成して、これらの積ｎ＝ｐｑと、（ｐ－１）および（ｑ－１）の最小公倍数Ｎと、この最小公倍数Ｎと互いに素な整数ｅに対し、$d_p = (1/e) \mod (p-1)$，$d_q = (1/e) \mod (q-1)$を満たすd_p，d_qと演算したときの、積ｎと整数ｅとを公開鍵とすると共に、素数ｐとｑおよび前記d_pとd_qとを秘密鍵とする鍵生成手段と、入力される平文の整数対を３次曲線上の点と対応させ、この点を前記公開鍵を用いてｅ倍した点を前記３次曲線上の演算で求め、この演算結果を暗号文として出力する暗号化演算手段とを有することを要旨とする。

【０００６】また、本願第２の発明は、素数ｐとｑとを生成して、これらの積ｎ＝ｐｑと、（ｐ－１）および

(3)

3

(q－1)の最小公倍数Nと、この最小公倍数Nと互いに素な整数eに対し、

$d_p = (1/e) \mod (p-1)$, $d_q = (1/e) \mod (q-1)$

を満たすd_p, d_qと演算したときの、積nと整数eとを公開鍵とすると共に、素数pとqおよび前記d_pとd_qとを秘密鍵とする鍵生成手段と、入力される暗号文の整数対を準同形変換した後に、法pのもとでd_p乗および法qのもとでd_q乗して、それらを中国人の剰余定理で合成して平文を出力する復号化演算手段とを有することを要旨とする。

【0007】また、本願第3の発明は、素数pとqとを生成して、これらの積n＝pqと、(p－1)および(q－1)の最小公倍数Nと、この最小公倍数Nと互いに素な整数eに対し、

$d_p = (1/e) \mod (p-1)$, $d_q = (1/e) \mod (q-1)$

を満たすd_p, d_qと演算したときの、積nと整数eとを公開鍵とすると共に、素数pとqおよび前記d_pとd_qとを秘密鍵とする鍵生成手段と、入力される平文の整数対を3次曲線上の点と対応させ、この点を前記公開鍵を用いてe倍した点を前記3次曲線上の演算で求め、この演算結果を暗号文として出力する暗号化演算手段と、入力される暗号文の整数対を準同形変換した後に、法pのもとでd_p乗および法qのもとでd_q乗して、それらを中国人の剰余定理で合成して平文を出力する復号化演算手段とを有することを要旨とする。

【0008】さらに、本願第4の発明は、送信元から送信される平文の整数対を3次曲線上の点と対応させ、これを送信元の公開鍵との乗算を当該3次曲線上の演算で行なって暗号化する暗号化手段と、この暗号化手段で暗号化された暗号文を前記送信元へ送信する送信手段と、この送信手段を介して送信された暗号文を受信する受信手段と、この受信手段を介して受信した暗号文に対し、自己の秘密鍵による巾乗算を行なって復号化する復号化手段とを有することを要旨とする。

【0009】

【作用】本発明によれば素数pとqとを生成して、これらの積n＝pqと、(p－1)および(q－1)の最小公倍数Nと、そのNと互いに素な整数eに対し、

$d_p = (1/e) \mod (p-1)$,

$d_q = (1/e) \mod (q-1)$

を満たすd_p, d_qとが鍵生成手段により演算されて、公開鍵nとeと、秘密鍵p，qおよびd_p，d_qとが作られ、入力文の整数対が3次曲線上の点に対応させられ、その各整数対に対して、公開鍵eにより3次曲線上で乗算され、あるいは秘密鍵d_pとd_qにより整数上でべき乗算されて、暗号化され、または復号化される。

【0010】

【実施例】以下、本発明に係る一実施例を図面を参照して

4

て説明する。図1は本発明に係る暗号・復号化装置の構成を示したブロック図である。

【0011】図1に示すように、データ読込み回路11は、鍵生成手段14および3次曲線加算回路17と接続される。この鍵生成手段14は、素数生成回路12と演算器13で構成され、それぞれデータ読込み回路11と接続されると共に素数生成回路12の出力は演算器13に接続される。また演算器13の出力は、第1のメモリ15に接続され、この第1のメモリ15の出力は3次曲線加算回路17と演算器20に接続される。第2のメモリ16の出力は3次曲線加算回路17に接続され、この3次曲線加算回路17の出力はデータ送信回路18に接続される。一方、データ受信回路19の出力は演算器20に接続され、さらにこの演算器20の出力はデータ送信回路18に接続される。

【0012】次に、図1を参照して本実施例の作用を説明する。データ読み込み回路11に大きな適当な素数生成の種sと、適当な小さい整数eと、送信しようとする平文とが入力される。これらのうち種sを用いて素数生成回路12で、素数pとqとが生成される。

【0013】その素数p，qと、データ読み込み回路11よりの整数eとが演算器13へ供給され、n＝pqの演算と、

$d_p = (1/e) \mod (p-1)$

$d_q = (1/e) \mod (q-1)$

の計算が行なわれる。通常はeの値として3または5を入力すればほとんどの場合よい。これら整数eと積nは公開鍵とされ、d_p，d_qは秘密鍵とされる。つまり素数生成回路12および演算器13は鍵生成手段14を構成している。秘密鍵d_p，d_q，p，qは第1のメモリ15に記憶される。

【0014】データ読み込み回路11よりの平文と、第2のメモリ16中の相手方、すなわち送信元の公開鍵e，nとが3次曲線加算回路17へ供給される。ここで平文の整数対(m_x，m_y)を3次曲線上の点と対応させ、その整数対に相手方の公開鍵eを3次曲線上の演算で乗算して暗号化する。つまり、特異な3次曲線$y^2 + axy = x^3$の上の整数対(x，y)を平文と対応させて演算する。

【0015】アフィン(affin)座標では、3次曲線上の2点、$P_1 = (x_1, y_1)$，$P_2 = (x_2, y_2)$が与えられたとき、これら2点の和$P_3 = P_1 + P_2$は次式で表される。

$P_1 \neq P_2$ のとき、

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

$\lambda = (y_2 - y_1) / (x_2 - x_1)$

$P_1 = P_2$ のとき、

$x_3 = \lambda^2 - 2x_1$

$y_3 = \lambda(x_1 - x_3) - y_1$

(4)

5

$\lambda = (3x_1^2 - ay_1) / (2y_1 + ax_1)$

この加算公式は斉次座標系でも同様に定義できる。これらの加算公式を繰り返し適用して、ある点Pの整数倍の点ePを求めることができる。つまり、5Pは(P＋P)と(4P＋4P)と(4P＋P)とにより求める。

【0016】したがって、e(m_x，m_y)は、例えば上記の加算公式を繰り返すことにより求められる。また整数対(m_x，m_y)が決まれば、これが位置する3次曲線(aの値)は自動的に与えられ、加算公式を提供できる。また、この演算は(mod n)で行ない、つまり加算値がnを越えると、その越えた方だけを加算結果とし

6

＊て計算する。このようにして3次曲線加算回路17で暗号化された整数対e(m_x，m_y)＝(c_x，c_y)は、暗号文としてデータ送信回路18により相手方へ送信される。

【0017】一方、データ受信回路19で受信された3次曲線上の点である暗号文(c_x，c_y) mod nは、まずmod pおよびmod qのもとでの1次元の暗号文c_pとc_qに変換する。

【0018】

【数1】

$$C_p = \frac{C_x^3}{C_y^2} \mod p, \qquad C_q = \frac{C_x^3}{C_y^2} \mod q \quad \cdots (1)$$

次に演算器20で各整数をd_p乗およびd_q乗して、1次元の平文m_pとm_qを計算する。

【0019】

【数2】

$$m_p = c_p^{dp} \mod p,$$
$$m_q = c_q^{dq} \mod q \quad \cdots (2)$$

このm_p，m_qとa_pとa_q

★★【数3】

但し、

$$a_p = \frac{C_x^8 - C_y^2}{C_x C_y} \mod p, \qquad a_q = \frac{C_x^8 - C_y^2}{C_x C_y} \mod q \quad \cdots (3)$$

から演算器20を用いて、それぞれ3次曲線上の整数対に変換する。

☆【0020】

☆【数4】

$$m_{xp} = \frac{a_p^2 m_p}{(m_p - 1)^2} \mod p, \qquad m_{yp} = \frac{m_{xp} a_p}{(m_p - 1)} \mod p.$$

$$m_{xq} = \frac{a_q^2 m_q}{(m_q - 1)^2} \mod q, \qquad m_{yq} = \frac{m_{xq} a_q}{(m_q - 1)} \mod q. \quad \cdots (4)$$

最期に中国人の剰余定理を用いて、m_{xp}mod pとm_{xq}mod qからm_x mod nを、m_{yp}mod pとm_{yq}mod qからm_y mod nを演算器20を用いて計算し、復号化された平文(m_x，m_y)が得られる。

【0021】次に、本発明に係る暗号システムの一実施例を図2を参照して説明する。利用者Aの暗号装置21と利用者Bの暗号装置22との間は通信線28で接続される。また、センタ装置23と暗号装置21との間は通信線24および送受信器26を介して接続され、センタ装置23と暗号装置22との間は通信線25および送受信器26を介して接続される。またセンタ装置23は、利用者の鍵が登録される鍵ファイル27を備えている。また、暗号装置21、22のそれぞれの構成は、図1に示した暗号装置とほぼ同一であり、対応する部分には同一符号を付してある。

【0022】まず、利用者Aの暗号装置21の鍵生成手段14で生成された公開鍵n_1，e_1は送受信器26より通信線24を通じてセンタ装置23内の鍵ファイル27に利用者Aの鍵として登録される。同様に利用者Bの暗号装置22の鍵生成手段14で生成された公開鍵n_2，e_2は送受信器26より通信線25を通じてセンタ装置23内の鍵ファイル27に利用者Bの鍵として登録される。

【0023】利用者Aが利用者Bへ通信文を暗号化して

送信する場合は、利用者Aは通信線２４を通じてセンタ装置２３から、利用者Bの公開鍵n_2，e_2を受け取り、前述した第１の実施例で示されるアルゴリズムに従って暗号化し、その暗号文の整数対を送信回路１８を通じて通信線２８へ送出する。

【００２４】利用者Bの暗号装置２２では、通信線２８から受信回路１９に受信された暗号文は、前記の通り復号化されて、元の平文が復元される。利用者Bから利用者Aへの暗号通信も同様に行なわれ、この場合は鍵n_1，e_1，d_{1p}，d_{2q}が用いられる。

【００２５】以上説明したように本実施例は、次の長所をもっている。

（１）本実施例の暗号方式は従来のＲＳＡ暗号に比べて、復号化速度が約２倍であり、暗号化速度はほぼ同じである。ＲＳＡ暗号は通常、復号に時間がかかっていたので、本実施例の方式では全体の速度向上が約２倍となっている。

（２）本実施例の暗号方式はＲＳＡ暗号と同じレベルの安全性をもつ。

【００２６】

【発明の効果】以上説明したように本発明は、従来のＲＳＡ暗号に比べたとき、復号化速度が約２倍と高速でありながら、暗号化速度及び安全性はほぼ同じであるという優れた効果を備える。

【図面の簡単な説明】

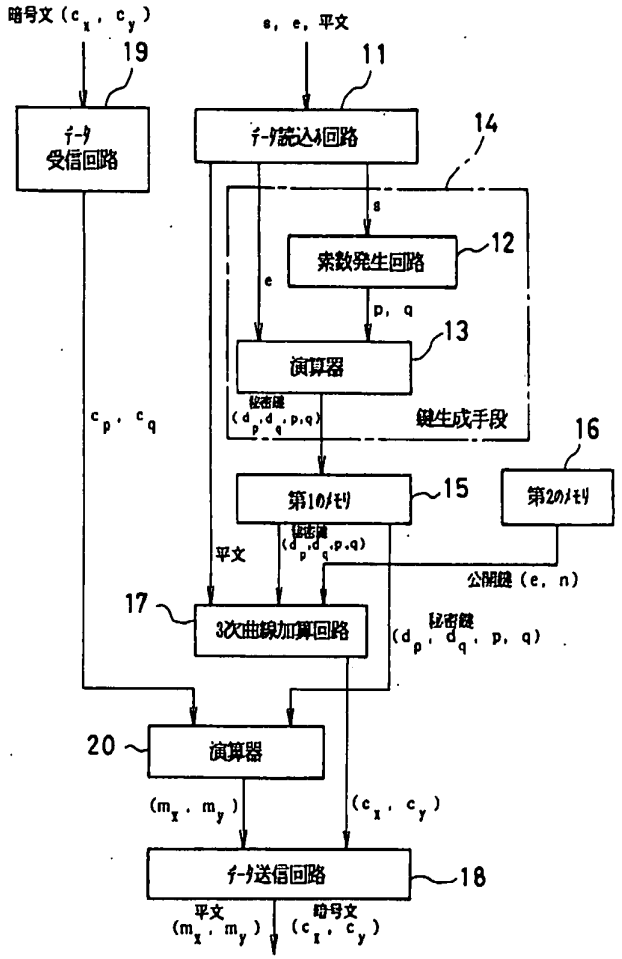
【図１】本発明に係る暗号装置の一実施例の概略の構成を示すブロック図である。

【図２】本発明に係る暗号システムの一実施例を示すブロック図である。

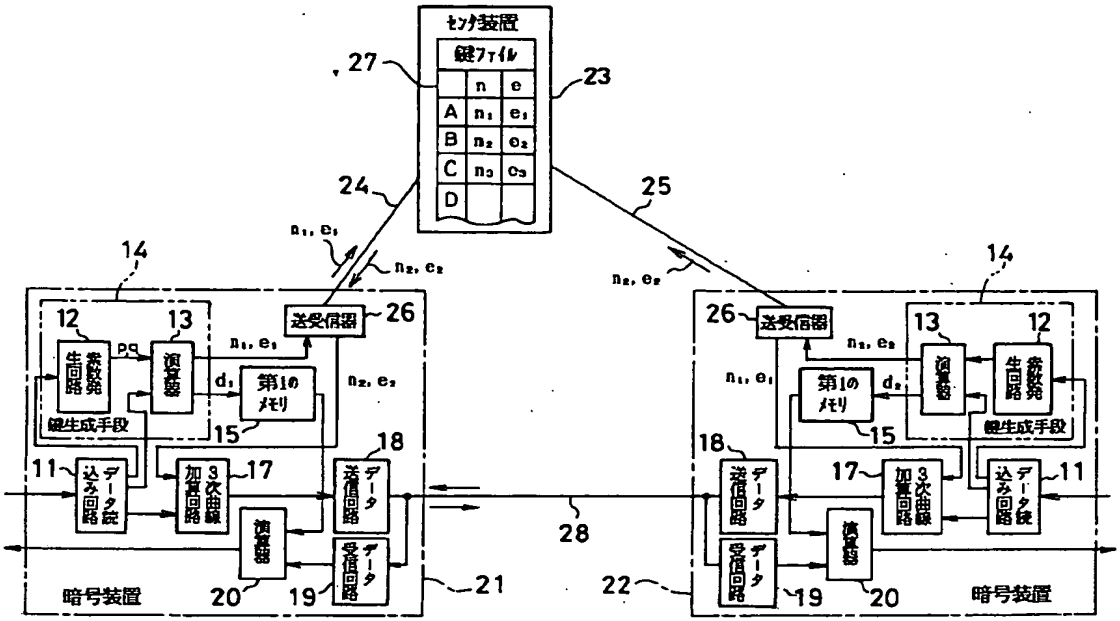
【符号の説明】

１１　データ読込み回路
１２　素数生成回路
１３　演算器
１４　鍵生成手段
１５　第１のメモリ
１６　第２のメモリ
１７　３次曲線加算回路
１８　データ送信回路
１９　データ受信回路
２０　演算器
２１　暗号装置
２２　暗号装置
２３　センタ装置
２４，２５，２８　通信線
２６　送受信器
２７　鍵ファイル

【図１】



【図2】


センタ装置
鍵ファイル
n
e
A
B
C
D
23
27
24
25
14
12
13
26
送受信器
乱数発生回路
演算器
第1のメモリ
鍵生成手段
15
11
データ読込み回路
3次曲線加算回路
17
18
データ送信回路
データ受信回路
19
20
21
22
28
暗号装置